



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/585,517	07/10/2006	Saar Wilf	2876/20	7666

7590 11/10/2009  
Mark M. Friedman  
c/o Polkinghorn  
9003 Florin Way  
Upper Marlboro, MD 20772

EXAMINER
----------

MACILWINEN, JOHN MOORE JAIN

ART UNIT	PAPER NUMBER
----------	--------------

2442

MAIL DATE	DELIVERY MODE
-----------	---------------

11/10/2009

PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

<b>Office Action Summary</b>	Application No. 10/585,517	Applicant(s) WILF ET AL.	
	Examiner John M. MacIwinen	Art Unit 2442	

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --**

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period **will** apply and **will** expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply **will**, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☐ Responsive to communication(s) filed on \_\_\_\_.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-50 is/are pending in the application.  
     4a) Of the above claim(s) \_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-50 is/are rejected.
- 7) ☒ Claim(s) 23 is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
     Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
     Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
     a) ☐ All    b) ☐ Some \* c) ☒ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_.
  3. ☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)            | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)   | Paper No(s)/Mail Date. ____.                                      |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date <u>12/04/2006</u> .  | 6) <input type="checkbox"/> Other: ____.                          |

## **DETAILED ACTION**

### ***Claim Objections***

1. Claim 23 objected to because of the following informalities: said claim lacks antecedent basis for the term "said parameter". Appropriate correction is required.

### ***Claim Rejections - 35 USC § 101***

2. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

3. Claim 1 – 50 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

4. Regarding claim(s) 1 – 43, said claims are rejected under 35 U.S.C. 101 as not falling within one of the four statutory categories of invention. While the claims recite a series of steps or acts to be performed, a statutory "process" under 35 U.S.C. 101 must (1) be tied to particular machine, or (2) transform underlying subject matter (such as an article or material) to a different state or thing. See page 10 of In Re Bilski 88 USPQ2d 1385. The instant claims are neither positively tied to a particular machine that accomplishes the claimed method steps nor transform underlying subject matter, and therefore do not qualify as a statutory process.

5. Regarding claim 44, said claim is directed to a system comprising a receiver and an analyzer. However, the limitations of claim 44 correspond to the limitations of claim 50; claim 50 being directed to computer software. Claim 50 thus provides evidence that

Art Unit: 2442

all the functionality of claim 21 is performed by code, and so the elements of claim 44 appear to be directed solely to software and thus non-statutory subject matter.

6. Additionally claims 44 – 49 appear to be directed to software based on the language in Applicant's specification; page 15 line 20 describing that the claimed elements "each . . . may be . . . software" and page 23 line 23 further describing the functionality of said claims performed by software.

7. Regarding claim 50, said claim is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter for failing to fall within one of the four categories of invention. Said claim is directed to "Computer software"; though the preamble recites a "computer-readable storage medium", a preamble is generally not accorded any patentable weight where the body of the claim does not depend on the preamble for completeness but, instead, the process steps or structural limitations are able to stand alone. See *In re Hirao*, 535 F.2d 67, 190 USPQ 15 (CCPA 1976) and *Kropa v. Robie*, 187 F.2d 150, 152, 88 USPQ 478, 481 (CCPA 1951).

### ***Claim Rejections - 35 USC § 112***

8. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

9. Claims 28 and 29 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Each of claims 28 and 29 recite a "round trip time gap"; after consulting Applicant's specification, it remains unclear what Applicant intends

Art Unit: 2442

to convey through the use of said term. In order to perform a complete examination, said term has been interpreted broadly.

***Claim Rejections - 35 USC § 103***

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

11. Claims 1 – 5, 8 – 20, 32, 37, 38, 41 and 43 – 50 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pazi (US 2003/0110274 A1) in view of Mackay (comp.os.ms-windows.networking.tcp-ip. "Can my ISP say if i'm using a proxy?" 2/16/2002. pgs. 1 - 4.).

12. Regarding claim 1, Pazi shows a method of making a determination, the method comprising:

a) receiving first and second information elements from the potential device, wherein the potential device is an original source of said second information element; and

b) determining whether a feature of an original source of said first information element and a feature of the potential device are features unlikely to relate to a single device,

wherein a positive result of said determining is indicative that the potential device is a device (Figs. 2, 3, [7-17]).

Art Unit: 2442

Pazi does not show where the determination is: whether potential relay device is a relay device.

Mackay shows making a determination whether a potential relay device is a relay device (pg. 2).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi with that of Mackay in order to best identify and understand the sources of received traffic and thus better control the types of traffic admitted to your network (Pazi, pg. 1 and pg. 2).

13. Regarding claim 2, Pazi in view of Mackay further show wherein said second information element is of a type that a relay device of a class of relay devices is unlikely to relay (Mackay, pg. 2).

14. Regarding claim 3, Pazi in view of Mackay further show wherein said class of relay devices is selected from the group consisting of a SOCKS proxy, an HTTP proxy using the GET method, an HTTP proxy using the CONNECT method, an IP router and a NAT device (Mackay, pg. 2).

15. Regarding claim 4, Pazi in view of Mackay further show wherein said second information element is part of a communication, wherein the communication is of a type selected from the group consisting of IP, TCP, ICMP, DNS, HTTP, SMTP, TLS, and SSL (Mackay, pg. 2).

16. Regarding claim 5, Pazi in view of Mackay further show wherein said first information element is part of a communication, wherein the communication is of a type

Art Unit: 2442

selected from the group consisting of IP, TCP, ICMP, DNS, HTTP, SMTP, TLS, and SSL (Mackay, pg. 2).

17. Regarding claim 8, Pazi in view of Mackay further show wherein said stage of determining comprises:

i) discovering said feature of an original source of said first information element; and

ii) discovering said feature of the potential relay device (Pazi, [47,55]).

18. Regarding claim 9, Pazi in view of Mackay further show wherein said stage of determining further comprises:

iii) comparing said feature of an original source of said first information element with said feature of the potential relay device (Pazi, [55]).

19. Regarding claim 10, Pazi in view of Mackay further show c) obtaining a parameter indicative of said feature of an original source of said first information element; and

d) obtaining a parameter indicative of said feature of the potential relay device (Pazi, [7-17] and Figs. 2, 3).

20. Regarding claim 11, Pazi in view of Mackay further show wherein said stage of determining further comprises:

iii) considering a time at which at least one of said feature of an original source of said first information element and said feature of the potential relay device, was discovered (Pazi, [44]).

Art Unit: 2442

21. Regarding claim 12, Pazi in view of Mackay further show c) obtaining a parameter indicative of a relationship between said feature of said original source of said first information element and said feature of the potential relay device (Pazi, [44, 50-52]).
22. Regarding claim 13, Pazi in view of Mackay further show wherein said stage of determining includes analyzing said parameter indicative of a relationship between said feature of said original source of said first information element and said feature of the potential relay device (Pazi, [44, 50-52]).
23. Regarding claim 14, Pazi in view of Mackay further show wherein said parameter is obtained from at least one of said first information element and said second information element (Pazi, [44, 50-52]).
24. Regarding claim 15, Pazi in view of Mackay further show c) sending an outgoing communication to at least one of said original source of said first information element and the potential relay device (Pazi, [16]); and
- d) Receiving a third information element from said at least one of said original source of said first information element and the potential relay device (Pazi, [16-18]).
25. Regarding claim 16, Pazi in view of Mackay further show e) deriving from said third information element information related to a feature of said at least one of said original source of said first information element and the potential relay device (Pazi, [16-18, 44, 49-52]).



Art Unit: 2442

26. Regarding claim 17, Pazi in view of Mackay further show iii) verifying that an original source of said third information element is said original source of said first information element (Pazi, [16-18, 47]).

27. Regarding claim 18, Pazi in view of Mackay further show iii) verifying that an original source of said third information element is the potential relay device (Pazi, [54]).

28. Regarding claim 19, Pazi in view of Mackay further show wherein said third information element is selected from the group consisting of an ICMP message, an ICMP Echo Reply message, a DNS query, an HTTP request, an HTTP response, an HTTP `Server` header, an IP address, a TCP port, a TCP Initial Sequence number, a TCP Initial Window, a WHOIS record, and a reverse DNS record (Mackay, pg. 2 and Pazi, [60-62]).

29. Regarding claim 20, Pazi in view of Mackay further show wherein at least one of said feature of an original source of said first information element and said feature of the potential relay device is a feature related to a configuration status (Mackay, pg. 2).

30. Regarding claim 32, Pazi in view of Mackay further show wherein at least one of said feature of an original source of said first information element and said feature of the potential relay device is selected from the group consisting of a sub-network, an administrator, and a location (Mackay, pgs. 1 – 2 and Pazi, [35]).

31. Regarding claim 37, Pazi shows a method of determining whether a potential device is a device, the method comprising:

a) sending a message to an information source device, triggering said information source device to send a DNS request;

Art Unit: 2442

b) determining from said DNS request whether said potential device is a device (Figs. 1, 2, [11-17]).

Pazi does not show where the determination is: whether potential relay device is a relay device.

Mackay shows making a determination whether a potential relay device is a relay device (pg. 2).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi with that of Mackay in order to best identify and understand the sources of received traffic and thus better control the types of traffic admitted to your network (Pazi, pg. 1 and pg. 2).

32. Regarding claim 38, Pazi shows a method of determining whether a potential relay is a device, the method comprising:

a) receiving first and second information elements from the potential device; and  
b) determining whether a feature of an original source of said first information element and a feature of an original source of said second information element are features unlikely to relate to a single device,

wherein a positive result of said determining is indicative that the potential device is a device (Figs. 2 and 3, [11-17]).

Pazi does not show where the determination is: whether potential relay device is a relay device.

Mackay shows making a determination whether a potential relay device is a relay device (pg. 2).

Art Unit: 2442

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi with that of Mackay in order to best identify and understand the sources of received traffic and thus better control the types of traffic admitted to your network (Pazi, pg. 1 and pg. 2).

33. Regarding claim 41, Pazi shows a method of determining whether a potential device is a device, the method comprising:

a) receiving first and second information elements from the potential device, wherein the potential device is an original source of said second information element; and

b) checking whether a location of the potential device is different than a location of an original source of said first information element (Figs. 2 and 3, [11-17]).

Pazi does not show where the determination is: whether potential relay device is a relay device.

Mackay shows making a determination whether a potential relay device is a relay device (pg. 2).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi with that of Mackay in order to best identify and understand the sources of received traffic and thus better control the types of traffic admitted to your network (Pazi, pg. 1 and pg. 2).

34. Regarding claim 43, Pazi shows a method of determining whether a potential device is a device, the method comprising:

a) determining whether a feature of an original source of a first information

Art Unit: 2442

element and a feature of the potential device are features unlikely to relate to a single device,

wherein the potential device is a transmitter of said first information element and of a second information element,

wherein the potential device is an original source of said second information element

wherein a positive result of said determining is indicative that the potential device is a device (Figs. 2 and 3, [11-17]).

Pazi does not show where the determination is: whether potential relay device is a relay device.

Mackay shows making a determination whether a potential relay device is a relay device (pg. 2).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi with that of Mackay in order to best identify and understand the sources of received traffic and thus better control the types of traffic admitted to your network (Pazi, pg. 1 and pg. 2).

35. Regarding claim 44, Pazi shows a system for determining whether a potential device is a device, the system comprising:

a) an information element receiver, for receiving information elements from a plurality of devices including an information source device and the potential device; and

b) a feature incompatibility analyzer, for determining whether a feature of said information source device and a feature of the potential device are features unlikely to

Art Unit: 2442

relate to a single device (Figs. 2 and 3, [11-17]).

Pazi does not show where the determination is: whether potential relay device is a relay device.

Mackay shows making a determination whether a potential relay device is a relay device (pg. 2).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi with that of Mackay in order to best identify and understand the sources of received traffic and thus better control the types of traffic admitted to your network (Pazi, pg. 1 and pg. 2).

36. Regarding claim 45, Pazi in view of Mackay further show c) a feature discovery module, for discovering at least one feature selected from the group consisting of a feature of said information source device and a feature of the potential relay device (Pazi, [55-58]).

37. Regarding claim 46, Pazi in view of Mackay further show wherein said information element receiver is further configured to receive information elements from a monitored host (Pazi, [55-58,61]).

38. Regarding claim 47, Pazi in view of Mackay further show c) an outgoing information element sender (Pazi, [61]).

39. Regarding claim 48, Pazi in view of Mackay further show c) a parameter obtainer, for obtaining at least one parameter selected from the group consisting of a parameter indicative of a feature of an information source device, a parameter indicative of a feature of the potential relay device, and a parameter indicative of whether a

Art Unit: 2442

feature of said information source device and a feature of said potential relay device are features unlikely to relate to a single device (Pazi, Figs. 2 and 3, [52]).

40. Regarding claim 49, Pazi in view of Mackay further show c) a feature database for storing a map between pairs of features and data indicative of whether said pairs of features are incompatible features (Pazi, [47,54]).

41. Regarding claim 50, Pazi in view of Mackay further show computer software, residing on a computer-readable storage medium, comprising instructions for causing a computer to:

- a) receive first and second information elements from a potential device, wherein the potential device is an original source of said second information element; and

- b) determine whether a feature of an original source of said first information element and a feature of said potential device are features unlikely to relate to a single device,

wherein a positive result of said determining is indicative that said potential device is a device (Figs. 2 and 3, [11-17]).

Pazi does not show where the determination is: whether potential relay device is a relay device.

Mackay shows making a determination whether a potential relay device is a relay device (pg. 2).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi with that of Mackay in order to best identify

Art Unit: 2442

and understand the sources of received traffic and thus better control the types of traffic admitted to your network (Pazi, pg. 1 and pg. 2).

42. Claims 6, 7 and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pazi in view of Mackay as applied to claim 1 above, and further in view of Reed (Applying the OSI Seven Layer Network Model to Information Security. November 21, 2003).

43. Regarding claim 6, Pazi in view of Mackay show claim 1.

Pazi in view of Mackay do not show wherein said first and said second information elements are parts of a single communication.

Reed shows wherein said first and said second information elements are parts of a single communication (Reed, pg. 24).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi in view of Mackay with that of Reed in order to exploit common knowledge relating to networking and information security (Reed, pg. 1).

44. Regarding claim 7, Pazi in view of Mackay and Reed show wherein said first and said second information elements are sent in two different layers of a protocol stack (Reed, pg. 24).

45. Regarding claim 33, Pazi in view of Mackay show claim 32.

Pazi in view of Mackay do not show wherein said determining includes examining a parameter indicative of at least one of said feature of a source of said first

Art Unit: 2442

communication and said feature of a source of said second communication, and said parameter is selected from the group consisting of an HTTP `User-Agent` header, an RFC 822 `X-Mailer` header, an RFC 822 `Received` header, an RFC 822 `Date` Header, an IP address, a WHOIS record, and a reverse DNS record.

Reed shows wherein said determining includes examining a parameter indicative of at least one of said feature of a source of said first communication and said feature of a source of said second communication, and said parameter is selected from the group consisting of an HTTP `User-Agent` header, an RFC 822 `X-Mailer` header, an RFC 822 `Received` header, an RFC 822 `Date` Header, an IP address, a WHOIS record, and a reverse DNS record (Reed, pgs. 23 – 24).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi in view of Mackay with that of Reed in order to exploit common knowledge relating to networking and information security (Reed, pg. 1).

46. Claims 21, 22, 23, and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pazi in view of Mackay as applied to claim 1 above, and further in view of Nilsen (alt.comp.lang.php. "how to detect PROXY?" 12/24/2001. pgs. 1-2).

47. Regarding claim 21, Pazi in view of Mackay show claim 1.

Pazi in view of Mackay do not show wherein said feature related to a configuration status is selected from the group consisting of an operating system type, an operating system version, a software type, an HTTP client type, an HTTP server



Art Unit: 2442

type, an SMTP client type, an SMTP server type, a time setting, a clock setting and a time zone setting.

Nilsen shows wherein said feature related to a configuration status is selected from the group consisting of an operating system type, an operating system version, a software type, an HTTP client type, an HTTP server type, an SMTP client type, an SMTP server type, a time setting, a clock setting and a time zone setting (pg. 1).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi in view of Mackay with that of Nilsen more frequently be able to identify device types (Nilsen, pg. 1).

48. Regarding claim 22, Pazi in view of Mackay and Nilsen further show wherein said determining includes examining a parameter indicative of said feature related to a configuration status (Nilsen, pg. 1).

49. Regarding claim 23, Pazi in view of Mackay and Nilsen further show wherein said parameter is selected from the group consisting of an HTTP 'User-Agent' header, an RFC 822 'X-Mailer' header, an RFC 822 'Received' header, an RFC 822 'Date' header, a protocol implementation manner, a TCP/IP stack fingerprint, an IP address, a TCP port, a TCP initial sequence number, a TCP initial window, a WHOIS record, and a reverse DNS record (Mackay, pg. 2)

50. Regarding claim 34, Pazi shows a method of determining whether a potential device is a relay device, the method comprising:

a) receiving first and second information elements from the potential device, wherein the potential device is an original source of said second information element;

Art Unit: 2442

and

b) analyzing a configuration status of an original source of at least one of said first and said second information elements (Pazi, [7-17]).

Pazi does not show where the determination is: whether potential relay device is a relay device.

Mackay shows making a determination whether a potential relay device is a relay device (pg. 2).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi with that of Mackay in order to best identify and understand the sources of received traffic and thus better control the types of traffic admitted to your network (Pazi, pg. 1 and pg. 2).

Pazi in view of Mackay do not show said configuration status selected from the group consisting of an operating system type, an operating system version, a software type, an HTTP client type, an HTTP server type, an SMTP client type, an SMTP server type, a time setting, a clock setting, and a time zone setting.

Nilsen shows said configuration status selected from the group consisting of an operating system type, an operating system version, a software type, an HTTP client type, an HTTP server type, an SMTP client type, an SMTP server type, a time setting, a clock setting, and a time zone setting (pg. 1).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi in view of Mackay with that of Nilsen more frequently be able to identify device types (Nilsen, pg. 1).

51. Claims 24 – 31, 35,36 and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pazi in view of Mackay as applied to claim 1 above, and further in view of Daude (US 6,892,235 B1).

52. Regarding claim 24, Pazi in view of Mackay show claim 1.

Pazi in view of Mackay do not explicitly show wherein at least one of said feature of a source of said first information element and said feature of the potential relay device is a feature related to communication performance.

Daude shows wherein at least one of said feature of a source of said first information element and said feature of the potential relay device is a feature related to communication performance (Abstract, Figs. 5 – 7).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi in view of Mackay with that of Daude in order to use automatic methods to analyze and better understand the network (Daude, Abstract.)

53. Regarding claim 25, Pazi in view of Mackay and Daude further show wherein said feature related to communication performance is selected from the group consisting of a measured communication performance, a measured relative communication performance, and an estimated communication performance (Daude, Figs. 5 – 7).

54. Regarding claim 26, Pazi in view of Mackay and Daude further show wherein said feature related to communication performance is selected from the group

Art Unit: 2442

consisting of a latency of communication, a latency of an incoming communication, a latency of an outgoing communication, a round trip time of a communication, a communication rate, an incoming communication rate, an outgoing communication rate, a maximum communication rate, an incoming maximum communication rate, and an outgoing maximum communication rate (Daude, col. 8 lines 36 – 40).

55. Regarding claim 27, Pazi in view of Mackay and Daude further show wherein said determining includes examining a parameter indicative of said feature related to communication performance (Pazi, [34]).

56. Regarding claim 28, Pazi in view of Mackay and Daude further show wherein said parameter is selected from the group consisting of time of receipt of an information element, time of sending of an information element, a round trip time, a round trip time gap, an IP address, a Whois record, a reverse DNS record, and a rate of acknowledged information (Daude, col. 8 lines 36 – 40).

57. Regarding claim 29, Pazi in view of Mackay and Daude further show wherein a higher round trip time gap is indicative of a higher likelihood that a relay device is being used for malicious purposes (Daude, col. 8 lines 60 – 65).

58. Regarding claim 30, Pazi in view of Mackay and Daude further show wherein said feature related to communication performance is estimated from information about at least one of said original source of said first communication and the potential relay device (Daude, Abstract).

59. Regarding claim 31, Pazi in view of Mackay and Daude further show wherein said information about at least one of said original source of said first communication

Art Unit: 2442

and the potential relay device is selected from the group consisting of a location of a device, a reverse DNS record of a device's IP address, and an administrator of a device (Daude, col. 11 lines 48 – 60).

60. Regarding claim 35, Pazi shows a method of determining whether a potential device is a device, the method comprising:

a) receiving first and second information elements from the potential device, wherein the potential device is an original source of said second information element (Pazi, [7-17], Figs. 1 and 2).

Pazi does not show where the determination is: whether potential relay device is a relay device.

Mackay shows making a determination whether a potential relay device is a relay device (pg. 2).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi with that of Mackay in order to best identify and understand the sources of received traffic and thus better control the types of traffic admitted to your network (Pazi, pg. 1 and pg. 2).

Pazi in view of Mackay do not show b) analyzing a feature related to communication performance of an original source of at least one of said first and said second information elements.

Daude shows b) analyzing a feature related to communication performance of an original source of at least one of said first and said second information elements (Abstract, Figs. 5 – 7).

Art Unit: 2442

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi in view of Mackay with that of Daude in order to use automatic methods to analyze and better understand the network (Daude, Abstract).

61. Regarding claim 36, Pazi in view of Mackay and Daude further show wherein said feature related to communication performance is selected from the group consisting of a latency of communication, a latency of an incoming communication, a latency of an outgoing communication, a round trip time of a communication, a communication rate, an incoming communication rate, an outgoing communication rate, a maximum communication rate, an incoming maximum communication rate, and an outgoing maximum communication rate (Daude, col. 8 lines 36 – 40).

62. Regarding claim 39, Pazi shows method of determining whether a potential device is a device, the method comprising:

a) receiving first and second information elements from the potential device, wherein the potential device is an original source of said second information element (Pazi, [7-17]).

b) checking whether an element related to the potential device is significantly different than an element related to to an original source of said first information element.

Pazi does not show where the determination is: whether potential relay device is a relay device.

Mackay shows making a determination whether a potential relay device is a relay

Art Unit: 2442

device (pg. 2).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi with that of Mackay in order to best identify and understand the sources of received traffic and thus better control the types of traffic admitted to your network (Pazi, pg. 1 and pg. 2).

Pazi in view of Mackay do not show checking round-trip times.

Daude shows checking round-trip times (Figs. 1, 4, 6 and col. 8 lines 25 – 65).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi in view of Mackay with that of Daude in order to use automatic methods to analyze and better understand the network (Daude, Abstract).

63. Claims 40 is rejected under 35 U.S.C. 103(a) as being unpatentable over Pazi in view of Mackay and Wilf (US 6,496,824 B1).

64. Regarding claim 40, Pazi shows a method of determining whether a potential device is a device, the method comprising:

a) receiving first and second information elements from the potential device, wherein the potential device is an original source of said second information element ([7-17]); and

b) checking whether a the potential device is different than the original source of said first information element ([7-17], Figs. 2 - 3).

Pazi does not show where the determination is: whether potential relay device is a relay device and checking an administrator.

Mackay shows making a determination whether a potential relay device is a relay device (pg. 2).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi with that of Mackay in order to best identify and understand the sources of received traffic and thus better control the types of traffic admitted to your network (Pazi, pg. 1 and pg. 2).

Pazi in view of Mackay do not show checking the operating system.

Wilf shows checking the operating system (Abstract, col. 4 lines 5 – 15).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi in view of Mackay with that of Wilf in order to fully utilize the information provided by network devices.

65. Claims 42 is rejected under 35 U.S.C. 103(a) as being unpatentable over Pazi in view of Mackay and Atsuki (US 2006/0146837 A1).

66. Regarding claim 42, Pazi shows a method of a method of making a determination, the method comprising:

a) receiving first and second information elements from potential device, wherein the potential device is an original source of said second information element; and

b) checking whether data from of the potential device is different than data from of an original source of said first information element (Figs. 1, 2 and [7-17]).



Art Unit: 2442

Pazi does not show where the determination is: whether potential relay device is a relay device and checking an administrator.

Mackay shows making a determination whether a potential relay device is a relay device (pg. 2).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi with that of Mackay in order to best identify and understand the sources of received traffic and thus better control the types of traffic admitted to your network (Pazi, pg. 1 and pg. 2).

Pazi in view of Mackay do not show checking an administrator.

Atsuki shows checking an administrator ([68-72]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Pazi in view of Mackay with that of Atsuki in order to utilize another piece of available data that can be used to identify devices (Atsuki, [70-72]).

### ***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to John M. MacIlwain whose telephone number is (571) 272-9686. The examiner can normally be reached on M-F 7:30AM - 5:00PM EST; off alternate Fridays.

Art Unit: 2442

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Joon Hwang can be reached on (571) 272 - 4036. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

John MacIlwinen

(571) 272 – 9686

/Joon H. Hwang/  
Supervisory Patent Examiner, Art Unit 2447